**SECURITY MODULE**

October 6, 1999
Last Updated March 14, 2002

# SWSS Project

USER REQUIREMENTS

# Table of Contents

# 1 INTRODUCTION

## 1.1 Purpose

**BUSINESS PROCESS and SWSS INTEGRATION**

SWSS (CPS) currently resides on local databases. The change to a statewide database necessitates changes in security and access.

## 1.2 Target Audience

Central Office Security Coordinators will have to add Local Office Security Coordinators and Local Office Security Coordinators will have to add users. First line Supervisors will have to submit the FIA 60 to the Local Security Coordinator to grant program/profile access for their employees.

The following personnel may also be interested:

- SWSS Trainers
- FIA Help Desk Personnel
- SWSS Advance Users
- SWSS Project Staff tasked with developing the User's Guide
- Zone Children's Services Specialists
- CFS Policy Staff
- Local Office Security Coordinators
- Central Office Security Coordinators
- Database Administrators

# 2 MODULE NARRATIVE

**Program Module Access**

A user must have permission to access a program module. Access is designated in the enrollment process. The modules are: adoption, foster care, juvenile justice, protective services, provider management, and security administration. A user may be limited or excluded from access to specific modules based on program requirements or management discretion. The system must require that modules be designated for each user upon enrollment and allow for changes.

**User name Assignment for "New Workers"**

1. New workers come into a county office.

2. Supervisor decides which security level (s), load number (s), alternate worker (optional), supervisor, and update capable program assignment (s) are to be assigned to the new worker. If the new worker is to be a security coordinator, the supervisor must decide how many counties and which county or counties the worker will need to cover.

3. Supervisor contacts his/her county security coordinator and requests access to SWSS for a new worker. Along with this request, the supervisor will also provide address, telephone, speaking language capabilities, load number (s), security level (s), alternate worker (optional), supervisor, and program assignment (s) information to the county security coordinator. If the supervisor is requesting his/her first security coordinator, supervisor may contact Central Office security administration directly. Only Central Office security coordinators are able to create other security coordinators.

4. County security coordinator (or supervisors) contacts Central Office security administrator and requests a unique username and/or initial password for the new worker for the SWSS application.

5. Central Office security administrator determines a unique username and/or initial password for the new worker's SWSS user account. The determination of the unique username is important because the current standard within the state government is to use the user's last name followed by their first initial. If this does not create a unique name digits are appended to the name until it is unique ("millerm7" for instance)[1].

6. The county security coordinator then runs the SWSS application. He/She activates the Utilities process, selects "Add Staff Profile", and creates the new user for the SWSS application. The creation process will specify the new worker's username, initial password, assigned load number (s), phone number, address, speaking language capabilities, security level (s), alternate worker (if one is assigned), supervisor, and update capable program assignment (s).

[1] The uniqueness of the username must be valid across the entire State of Michigan. If it is done correctly, this information can also be coordinated with UNIX usernames as well as GroupWise usernames in order to facilitate a "single user sign-on". The procedure for determining unique SWSS usernames is outside the scope of the SWSS application itself.

7. The county security coordinator then informs either the new worker or the worker's supervisor that the new SWSS account has been created. The username and/or initial password is then passed on to the new worker along with instructions that the initial password should be changed the first time he/she logs into the system. The new worker must also be informed of the load number (s) that have been assigned to him/her.

8. The new worker's supervisor will then make certain that the worker's computer has the SWSS application correctly installed. The new worker is now ready to begin using the SWSS application.

9. The security coordinator must be provided the ability for Financial Specialists to be enrolled in to SWSS Security Profile.

# 3 NAVIGATION FLOW

3.1

**Central Office Security Administration**

**PROCESSES**

**Adding a Local Office Security Coordinator**

The Central Office Security Administrator will have certain access that will be restricted to Central Office Security Administration only. Central Office Administrators can make any changes that a Local Office security coordinator can make in any county/district settings statewide. The Central Office security administrator has "superuser" status.

The Central Office Security administrator will enroll local office security administrators by having the security officers complete the FIA-60 (Service Worker Support System security form). This form can be accessed as a Microsoft Word template. The Central Office security administrator can enroll/deactivate the local office security coordinator in more than one county or district. This function is reserved only for Central Office. The Central Office security administrator must enter the SWSS security profiling in the following manner:

**Changing Local Office Security Coordinators/Passwords**

The local office security coordinator will need to be able to change his/her password and the passwords for those users in their office, and to inactivate staff profiles for users in their office. Central office security administration must be able to enroll and deactivate the local office security coordinators.

## 3.2 System Flow

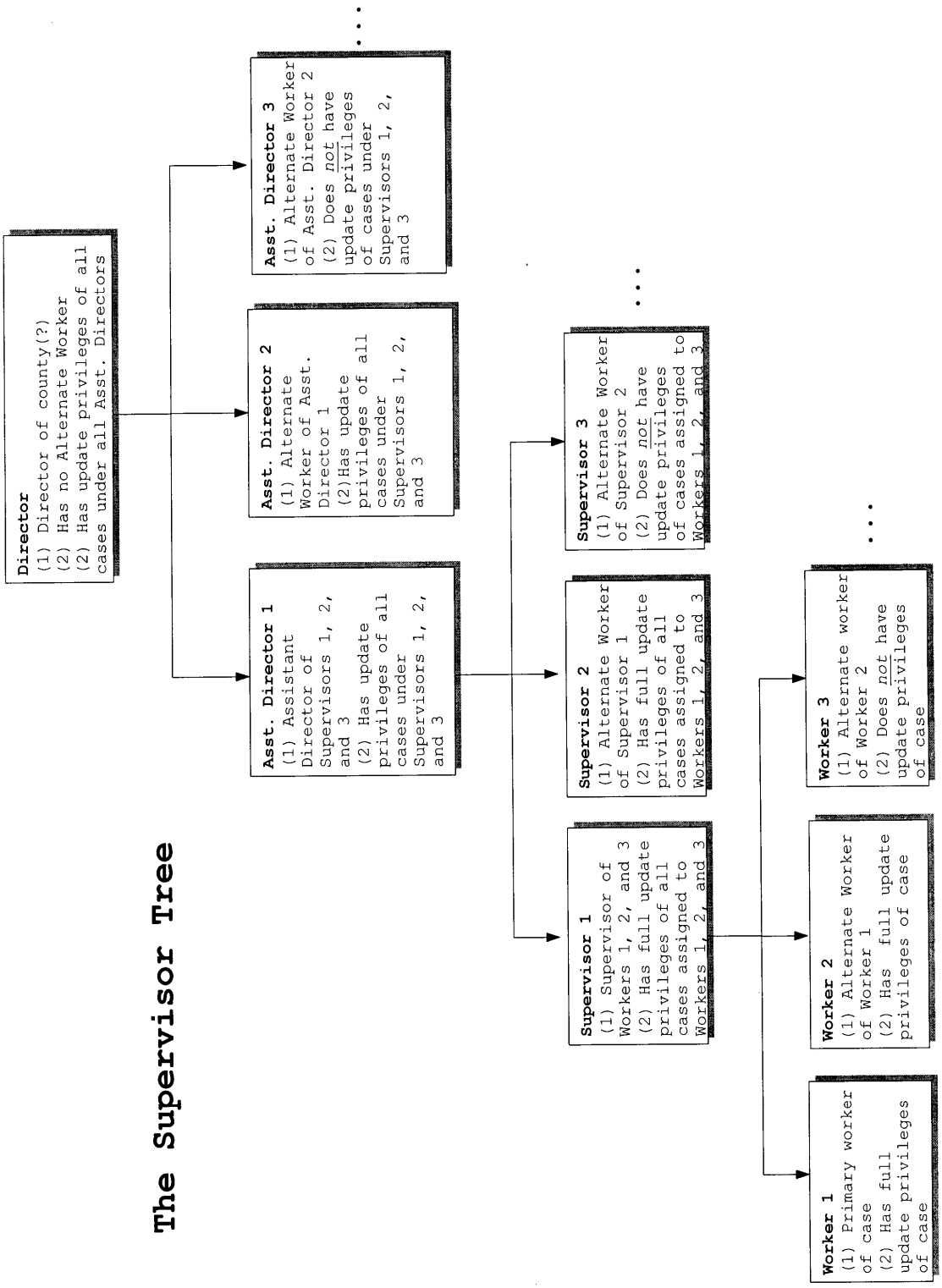
System flow is effected by :

**Access:** Access is determined by four things:

1. Supervisor tree
2. Location (county, dual county, state)
3. Level/function (clerical, caseworker, first-line supervisor, second-line supervisor, third-line supervisor, top level administrator, specialist)
4. Program module (CPS, adoption, foster care, juvenile justice, prevention, and provider management.)

**Supervisor Tree**

The supervisor tree determines if a user has file update privileges. To update an existing case, a user must be the assigned worker or alternate; assigned supervisor or alternate; or, assigned manager or alternate. Other users have read only access with some exceptions.


The Supervisor Tree
Director
(1) Director of county(?)
(2) Has no Alternate Worker
(2) Has update privileges of all cases under all Asst. Directors
Asst. Director 1
(1) Assistant Director of Supervisors 1, 2, and 3
(2) Has update privileges of all cases under Supervisors 1, 2, and 3
Asst. Director 2
(1) Alternate Worker of Asst. Director 1
(2)Has update privileges of all cases under Supervisors 1, 2, and 3
Asst. Director 3
(1) Alternate Worker of Asst. Director 2
(2) Does not have update privileges of cases under Supervisors 1, 2, and 3
Supervisor 1
(1) Supervisor of Workers 1, 2, and 3
(2) Has full update privileges of all cases assigned to Workers 1, 2, and 3
Supervisor 2
(1) Alternate Worker of Supervisor 1
(2) Has full update privileges of all cases assigned to Workers 1, 2, and 3
Supervisor 3
(1) Alternate Worker of Supervisor 2
(2) Does not have update privileges of cases assigned to Workers 1, 2, and 3
Worker 1
(1) Primary worker of case
(2) Has full update privileges of case
Worker 2
(1) Alternate Worker of Worker 1
(2) Has full update privileges of case
Worker 3
(1) Alternate worker of Worker 2
(2) Does not have update privileges of case

Clerical staff: **need some definitions here**

Designated individuals in the program offices may have specific update privileges for efficient program support. These updating privileges need to be worked out with systems development staff.

The local system administrator would not have case update privileges.

**Location**

In general, a user's location will be limited to one county. However, some users will have dual or multiple county responsibilities. Therefore, the system must be able to reflect multi-county or even statewide responsibility. Examples are: workers, supervisors and managers in dual county arrangements; adoption staff with multiple county areas; program office staff with statewide responsibility.

**Level/Function**

A user's level or function determines the extent of update privileges. Clerical level users have access to and update privileges for all cases in their unit except for high profile cases. Workers have update privileges for current data fields but may not change history or closed cases. Supervisor, managers and designated program office users may change closed cases and history. The local system administrator would have access to utility functions but would not have case update privileges.

Statewide read-only access must be available to all users including those who have no update privileges, such as zone office specialists. A read-only user level must be created to provide access to users who have no update privileges.

**Program Module Access**

A user must have permission to access a program module. Access is designated in the enrollment process. The modules are: adoption, foster care, juvenile justice, protective services, provider management, and security administration. A user may be limited or excluded from access to specific modules based on program requirements or management discretion. The system must require that modules be designated for each user upon enrollment and allow for changes.

# 4 REQUIREMENTS LIST

The comprehensive (we hope) list of requirements derived from the original requirements, ensuing memos, emails, and test plan documentation.

## 4.1 Screen, Data, Out-of-Module, Output, Out-of-Module and Miscellaneous Requirements

The following requirements were derived from the original requirements documents written by policy staff for the SWSS project. Any ensuing memos, emails, or test plans regarding the project were also searched. It is intended to be a comprehensive list of all requirements pertaining to the Security "module"[2]. Each individual requirement has a unique identifier; the two letter prefix identifies this particular module (SC = security).

The list is to be used in a Requirements Traceability Matrix, which will be comprised of all the requirements for all the SWSS modules, so that the status of each requirement can be tracked and verified.

**SC-1 SCREEN REQUIREMENTS:**

SC-1.1.1 This module addresses security concerns shared by almost all SWSS screens.

**SC-2 DATA EDITING REQUIREMENTS:**

SC-2.1 See **MODULE REQUIREMENTS**

**SC-3 OUT-OF-MODULE REQUIREMENTS:**

SC-3.1 Login must detect another instance of any of the SWSS modules and display a message informing the user that they must halt the other running SWSS application before logging in. (See LO-4.4)

**SC-4 MODULE REQUIREMENTS:**

SC-4.1.1 All valid SWSS users must be assigned a load number. (See UT-3.4.1)

SC-4.1.1.1 Financial Specialist will only be assigned a load number (this load number will work as an identification or designation for a Financial Specialist) for the district/districts within a county or counties that they are responsible for.

SC-4.1.1.2 There is only one exception. Users who are Central Office Security Coordinators do not need a load number. (See UT-1.8.2.2 and UT-3.4.1.1)

SC-4.1.1.3 There must be a method of creating valid SWSS staff profiles and assigning valid load numbers to those profiles. (See the "Utilities User Requirements.doc" document for more information) (See UT-1.4)

[2] Security is not a module in itself, but a collection of business rules that must be enforced within all the SWSS applications modules.

SC-4.2 Central Office needs inquiry access for case information. (See UT-3.4.2)

SC-4.2.1 Provide the ability for Financial Specialists to be enrolled and profiled in to SWSS Security Profile.

SC-4.3 There must be a mechanism to create a SWSS username that accepts usernames generated by the State of Michigan's controlling authority[3] on usernames. (See UT-2.1.3 for username info. See DMB's CNOC for info on a controlling authority.)

SC-4.4 SWSS LOGIN REQUIREMENTS:

SC-4.4.1 The user must be a Security Coordinator in order to Add or Inactivate staff profiles. (See UT-1.11 and UT-1.11.1)

SC-4.4.2 When a Security Coordinator changes a profile's password, the user of that profile must be forced to change his/her password the next time he/she logs into SWSS. (See LO-4.3.2)

SC-4.4.3 When a user logs into SWSS the first time after their profile is created, the user must be required to change his/her password before allowing entry into SWSS. (See LO-4.3.1)

SC-4.4.4 If a user incorrectly types his/her password three times, the application must lock the user out of SWSS and require that a security coordinator unlock his/her password. This must be accomplished by requesting that a security coordinator reset the user's password to a different value. (See LO-4.3.4)

SC-4.5 COMMON REQUIREMENTS:

SC-4.5.1 After thirty minutes of idle time, the SWSS application must be disconnected from the Oracle database. (See CM-3.1.1 and UT-3.5.1)

SC-4.5.1.1 If the user returns to the workstation and performs an action upon the database, the SWSS application must prompt the user to reestablish (reverify) his/her identity. This must be implemented in all SWSS modules that access the database. (See CM-3.1.1.1 and UT-3.5.1.1)

SC-4.5.2 Restrict users to one single session on the SWSS application, i.e., don't allow a single username to sign into SWSS from two different computers[3]. This is to be implemented with the database as part of the Oracle user profile.

SC-4.5.3 All password fields must disguise password entries by displaying asterisk ("*") characters instead of what the user actually types in. (See LO-2.1.1)

SC-4.5.4 Deleted.

SC-4.5.5 If a period of more than 90 days passes before a user changes his/her password, the password must expire. This must force the user to change his/her password the next time the user logs in. (See LO-4.3.3)

[3] Whatever that is

SC-4.5.6 The SWSS application must lock out any user after three months (90 days) of user inactivity[4]. This must then force the user to request that a Security Coordinator "unlock" his/her account by changing the user's password. (See LO-4.6)

SC-4.5.7 Users must be able to change their own passwords. (See UT-4.7)

SC-4.5.7.1 When the user resets their own password, do not allow him/her to set it to a value that has been used within the last three password changes. This is to be implemented with the database as part of the Oracle user profile. (Also see UT-4.6.1 and LO-2.1.6)

SC-4.5.8 The county number assigned to the Central Office is 84. (This must be used throughout SWSS; i.e., every other module must be aware of it.)

SC-4.5.9 No two users may have the same load number. (See UT-4.8)

SC-4.6 SECURITY TO GRANT ACCESS TO SWSS MODULES:

SC-4.6.1 If the Main Menu module is accessing any of these modules, the current circumstances of the selected case and the current user must allow access to the module up to this point. All modules commonly do these security checks whenever they try to access one another.

SC-4.6.2 M.A.R.E. REGISTRATION:

SC-4.6.2.1 The current user must be denied access to MARE if the selected case's legal status is "Court Ward Supervised Adoption" (43) or "OTI-Adoption" (49)

SC-4.6.2.1.1 If the currently selected case does have a legal status of "Court Ward Supervised Adoption" (43) or "OTI-Adoption" (49), then the information message must state "Access to M.A.R.E. is denied; child is already in an adoptive placement."

SC-4.6.2.2 The current user must be granted access to MARE if the current legal status assigned to the selected case is either "Permanent Court Ward" (41), "MCI Ward" (44) or "Dual Ward*" (52, 91, 93, 94*) ***and*** the goal code assigned to the case is "Adoption" (10).

SC-4.6.2.2.1 The message must state "Access to M.A.R.E. is denied; the goal for this ward is not adoption."

SC-4.6.2.3 The current user must be granted access to MARE regardless of the legal status if the case state is currently "Active-As" (250) or "Registered-As" (275) ***and*** the goal code assigned to the case is "Adoption" (10).

SC-4.6.2.3.1 The message must state "Access to M.A.R.E. is denied; this temporary ward's case has not been assigned to an adoption worker."

SC-4.6.2.4 If the current user is denied access to MARE, the application must display a message stating that access to the s elected module is denied. This message must also specify why access was denied.

[4] User inactivity is defined, as the user has not logged into SWSS for three months.

SC-4.6.3 CASE REGISTRATION:

SC-4.6.3.1 The current user must be denied access to the Case Registration module if the current case state is “Active” (200), “Active-As” (250) , “Active-R” (450), “Closed” (600), or “Withdrawn” (800).

SC-4.6.3.2 The user must also be denied access to “Case Registration” if the user attempts to access it from the Utilities module.

SC-4.6.3.3 The requirements in the Soundex module may override these requirements. See the documentation for that module for more information.

SC-4.6.4 The user must be denied access to the “Funding Determination” module if the legal status currently assigned to the selected case is “OTI-Delinquent” (47), “OTI-Neglect” (48), “OTI-Adoption” (49), “Non-Ward-Del Petition Filed” (50).

SC-4.6.4.1 If the legal status of the selected case is Court Ward Supervised Adoption, the user must be permitted ‘view only’ access to the Funding Determination Module.

SC-4.6.5 The user must be granted access to the Legal module if the selected case has been assigned to “Foster Care”, “Adoption”, or “Juvenile Justice”; otherwise, the user must be denied access to the Legal module.

SC-4.6.6 Access to the Payment module must be view only if the selected case has been assigned one of the following legal status codes: ‘Court Ward Supervised Adoption’ (43), ‘OTI-Delinquent’ (47), ‘OTI-Neglect’ (48), ‘OTI-Adoption’ (49), or ‘Non-Ward Delinquent Petition Filed’ (50).

SC-4.6.6.1 Access to the Payment module must be view only if the current case state is not one of the following: ‘Active’ (200), ‘Active-As’ (250), or ‘Active-R’ (450).

SC-4.6.6.2 If the case is closed (case state = ‘Closed’ (600)), the worker’s supervisor(s) have update capability. Other users can view only.

SC-4.6.7 The user must be granted access to the CPS Transfer module if the selected case is currently in an “Unregistered” (400) state and has been assigned to the “Foster Care” program

SC-4.6.8 If the selected case is “Unregistered” (400) the user must be denied access to the following modules: Child info, Member info, Legal info, Funding determination, Placement, Medicaid, Payments, Five day packet, Education, Case Closing, Print-133a, Print-5S

SC-4.7 MAIN MENU/UTILITIES REQUIREMENTS:

SC-4.7.1 If the user is in the Utilities module and he/she is a PROGRAM OFFICE OR P/DC user accessing the Payment Document Control utility or the P/DC Modification action, a Central Office Security Coordinator or a Local Office Security Coordinator, then leaving the Utilities module must end his/her SWSS session. (See UT-1.2.1 and UT-1.2.2)

SC-4.8 HIGH PROFILE CASE REQUIREMENTS:

SC-4.8.1 If the current case has been flagged as "high profile"[5] then only the assigned worker or that worker's supervisory chain of command may have access to any applicable modules for that case. Information contained in the Case Summary module is the only case specific information any other user may view.

SC-4.8.1.1 There is one exception. A PROGRAM OFFICE OR P/DC user must be allowed access to the Payments Online! Module when s/he enters the log numbers of a confidential case from the Utilities module (after selecting the P/DC Modification action).

SC-4.9 USER LEVEL ACCESS PRIVILEGES

SC-4.9.1 Worker-level users have access to create cases, add case data to the appropriate modules, to register, open, and close the cases.

SC-4.9.2 Unit-Clerk level users have access to update any case in that user's unit except for high-profile cases. (See MM-4.6 and UT-4.3)

SC-4.9.3 Supervisor level users have access to create cases, assign cases to workers under their supervision, to register, open, close, withdraw, and delete cases assigned to their own load number or to any case assigned to a worker under their supervision.

SC-4.9.4 Deleted.

SC-4.9.5 Central office security coordinators can enroll local office security coordinators, reset username passwords, change passwords, and inactivate user profiles, but can not view any case data. (See UT-1.7 through UT-1.11.5.1)

SC-4.9.6 Local office security coordinators can enroll users within their local office, can reset username passwords, change passwords, and inactivate user profiles. See UT-1.7 through UT-1.11.5.1)

SC-4.9.6.1 A local office security coordinator cannot have access to any other SWSS program under that unique user name. (See UT-1.5.3.2)

SC-4.9.6.1.1 Once a user name is designated as a security administrator or a PROGRAM OFFICE OR P/DC user accessing the Payment Document Control utility, that user name is restricted to one load number. (See UT-1.5.3.2.1 and UT-1.5.1.5.2)

SC-4.9.7 PROGRAM OFFICE OR P/DC users accessing the Payment Document Control utility (or the P/DC Modification action) are only allowed access to the Login Module, Utilities Module, the Payments Module, and the Payment Document Control utility under this unique user name. These users cannot have access to any other SWSS module. These users use the Utilities module to change their own password and access the Payment Document Control utility or the P/DC Modification action (the Payments Module) from the Choose Action menu in the Utilities module. (See PON-3.3.1, and LO-4.5.1)

[5] Cases in which the parties involved are notorious or infamous for any of a variety of reasons, and therefore it is in MFIA's best interests to restrict access to the case.

SC-4.10 If the user performs an action upon the database after the database has timed the user out, SWSS must automatically reconnect to the database and continue working.

SC-4.11 Central Office users (county 84) need inquiry access for case information.

SC-4.12 Payments ONLINE! REQUIREMENTS

SC-4.12.1 Deleted

SC-4.12.2 PROGRAM OFFICE OR P/DC users must not be permitted to become SWSS Security Coordinators under this unique user name.

**SC-5 OUTPUT REQUIREMENTS:**

SC-5.1 The Security module refers to the usage of the "Appointment of LOA2/SWSS Staff Profile Coordinator" form and the "FIA-60 SWSS Profile/Security Agreement" form. These forms must be filled out by hand and are not electronically generated by SWSS.

**SC-6 MISCELLANEOUS REQUIREMENTS:**

# 5 EXAMPLE OUTPUT

Gather and include the forms and letters generated by this module. If possible, mark up the examples to explain the data fields to show the source or whether or not it is required.

None.

# 6 DATA ELEMENT DESCRIPTIONS

A table of all the data elements entered within this module. For each item, describe its range of acceptable values. Designate items as being required for ASSIST, CIS, LICENSING or AFCARS (and any combination thereof). Also describe what other modules check these values.

Show validation tables of combinations of data. Are there data dependencies?

# 7 HELP MESSAGES

There are to be three levels of help available: Screen, which describes how the process for the current module is supposed to work, Context-Sensitive, which describes a particular data field on the screen, and Status Panel, which offer hints about the field or command button with the current focus.

7.1 SCREEN (Section or Module level. Offers an entry point to the big help file.)

7.2 CONTEXT-SENSITIVE ("F1", aka "detail")

7.3 STATUS PANEL MESSAGES (formerly known as "Field Level" and "Baby" before that.)

## Module: Security

| Field | *New Message* |
|---|---|
| SSN | Enter social security number (999-99-9999) |
| Application | Select application type |
| Worker | Select worker |
| (Name) | (panel title) |
| Last | Enter last name |
| Suffix | Enter suffix |
| First | Enter first name |
| Middle | Enter middle initial |
| UserName | Enter username |
| County | Select county |
| District | Select district |
| Section | Enter section number |
| Unit | Enter unit number |
| Worker | Enter worker number |
| Worker Security Level | Select worker security level |
| Phone | Enter area code and telephone number |
| Ext. | Enter extension |
| Hours 1 | no message |
| Hours 2 | no message |
| (Password) | (panel title) |
| Old | Enter old/current password |
| New | Enter new password ( 6 to 8 characters) |
| Confirm | Re-enter new password to confirm |
| Choose Action Screen | Select to go back to Staff Utilities |
| Next>> | Select to go to next screen |
| (Worker Update Access) | (panel title) |
| Protective Services | Select all that apply |
| Child Foster Care | Select all that apply |
| Adoption | Select all that apply |
| Juvenile Justice | Select all that apply |
| Provider Management | Select all that apply |

| | |
|---|---|
| Security Administration | Select all that apply |
| (Worker Relationships) | (panel title) |
| Alternate | Select alternate worker |
| Supervisor | Select supervisor |
| (Adoption Supervisor County Assignments) | (panel title) |
| Counties Available | Select county |
| Counties Assigned | Select county |
| Add > | Select to add highlighted county to list |
| < Remove | Select to remove highlighted county from list |
| <<Previous | Select to go back without saving changes |
| Next>> | Select to go to next screen |
| (Primary) | (panel title) |
| (Address) | (panel title) |
| Line 1 | Enter street address |
| Line 2 | Enter supplemental address |
| City | Enter city |
| State | Select state |
| Zipcode | Enter zip code |
| Zip + 4 | Enter additonal 4 digits, if known |
| E-Mail | Enter e-mail address |
| <County Addr. | Select to enter county address |
| Copy> | Select to copy address |
| County Addr. > | Select to enter county address |
| (Mailing) | (panel title) |
| (Address) | (panel title) |
| Line 1 | Enter street address |
| Line 2 | Enter supplemental address |
| City | Enter city |
| State | Select state |
| Zipcode | Enter zip code |
| Zip + 4 | Enter additonal 4 digits, if known |
| E-Mail | Enter e-mail address |
| (Phones) | (panel title) |
| Fax | Enter fax area code and telephone number |
| Ext. | Enter extension |
| (Languages) | (panel title) |
| (drop down list) | Select language |
| (drop down list) | Select language |
| (drop down list) | Select language |
| <<Previous | Select to go back without saving changes |
| Next>> | Select to go to next screen |
| (Security Coordinator County-District Assignments) | (panel title) |
| List of Counties | Select county |
| List of County Districts | Select county districts |
| Add | Select to add highlighted county and county districts to list |
| County-District Assignments | Select county-district assignments |
| Remove | Select to remove highlighted county and county district assignments from list |
| LOA2 Worker | no message |
| <<Previous | Select to go back without saving changes |
| Continue | Select to go to next screen |

# 8 MODULE DEPENDENCIES

Security is dependent upon Log In to identify the user and their status. Security provides access to different functions based on the user profile entered in Utilities.

# 9 SCENARIOS

The requirements scenarios that call for data entered by this module. This is just a cross reference into the

# 10 TEST PLANS

The updated test plans written by the Program Office and/or the developer to verify the correctness of the finished application.

# 11 SOURCE MATERIAL

The following items are included for historical purposes only. The current requirements were derived from this source material, and are, in places, out of date, incorrect, or conflicting.

## 11.1 Original Requirement

**CHILDREN'S *SWSS***
**REQUIREMENTS FORM**

| | |
|---|---|
| **Assigned Policy Analyst:** | **Lee Hunsberger** |
| **Date Received By BuIS:** | |
| **Requirement #** (from BuIS)**:** | |

Security, Access Levels

**1. BUSINESS PROCESS and 2. SWSS INTEGRATION.** SWSS currently resides on local databases. The change to a statewide database necessitates changes in security and access.

Security

Only enrolled users can have access. Supervisor must authorize each user and provide information to the local security coordinator. Required information includes worker number, alternate number, supervisor number, user level, language(s), worker name, work address and phone number, and the application modules to which this user will have access.

Local security coordinator or alternate enrolls user locally. Since this is a statewide system, the local security coordinator must contact the statewide database administrator (DBA) to enroll new user. Consistent with other statewide systems such as e-mail , the database administrator will assign a unique user identification and password. Local security coordinator must contact DBA to report inactivated users.

Users must be able to change passwords. Local coordinators should be able to change supervisor, alternate, security level, name, address, phone and program access. DBA must reset passwords and inactivate unique user identifications.

Users with multiple county responsibility would be enrolled by the security coordinator who would handle CIS access for them.

Access

Access is determined by four things:
Supervisor tree
Location (county, dual county, state)
Level/function (clerical, caseworker, first-line supervisor, second-line supervisor, third-line supervisor, top level administrator, specialist)
Program module (CPS, adoption, foster care juvenile justice, prevention, licensing, provider management)

Supervisor Tree

The supervisor tree determines if a user has file update privileges. To update an existing case, a user must be the assigned worker or alternate; assigned supervisor or alternate; or, assigned manager or alternate. Other users have read only access with some exceptions.

Clerical staff need limited update ability to add, change or delete case numbers and recipient identification numbers. Clerical staff also needs access to some narrative sections. However, these staff aren't in the supervisor tree; i.e. clerical staff are neither the assigned worker nor alternate. There needs to be a way to allow clerical update access to cases for which they are not the worker or alternate.

Designated individuals in the program offices may have specific update privileges for efficient program support. These updating privileges need to be worked out with systems development staff.

The local system administrator or alternate would not have case update privileges.

Location

In general, a user's location will be limited to one county. However, some users may be have dual or multiple county responsibilities. Therefore, the system must be able to reflect multi-county or even statewide responsibility. Examples are: workers, supervisors and managers in dual-county arrangements; adoption staff with multiple county areas; program office staff with statewide responsibility.

Level/Function

A user's level or function determines the extent of update privileges. Clerical level is limited to accessing case number and recipient identification number fields as well as specified narrative sections. Workers have update privileges for current data fields but may not change history or closed cases. Supervisors, managers and designated program office users may changed closed cases and history. The local system administrator or alternate would have access to utilities functions but would not have case update privileges.

Statewide read-only access must be available to all users including those who have no update privileges, such as zone office specialists. A read-only user level must be created to provide access to users who have no update privileges.

Program Module Access

A user must have permission to access a program module. Access is designated in the enrollment process. The modules are (will be): adoption, foster care, juvenile justice, protective services, provider management, security administration. A user may be limited or excluded from access to specific modules based on program requirements or management discretion. The system must require that modules be designated for each user upon enrollment and allow for changes.

**3. DATA ELEMENTS.** To be determined with development staff.

**4. EDITS.** To be determined with development staff.

**5. OUTPUTS.** To be determined with development staff.

**6. TRAINING ISSUES***. To be determined with development staff.

**7. TESTING ISSUES***. To be determined with development staff.

**8. DEPENDENCIES.** To be determined with development staff.

**9. SIGNATURES**

| | Signature | Date |
|---|---|---|
| **Policy Analyst:** | | |
| **Policy Supervisor:** | | |
| **BuIS Analyst:** | | |

*Revised on 11/20/96

## 11.2 Memos and E-mails

### 11.2.1 Addendum 1

**STATE OF MICHIGAN**
**FAMILY INDEPENDENCE AGENCY**

**MEMORANDUM**

**To:** Sue London, Director
SWSS Project

Date: January 6, 2000

**From:** Mary Ann Jensen, Consultant
SWSS Policy
Child and Family Services Adminstration

**Subject:** Security Module Documentation - Addendum 1

Based on discussions with development staff, it is necessary to amend the November 1, 1999 memo on the Security Module. The following revision is necessary:

SC-4.6.2.2 must be revised to include the Dual Legal Statuses 91, 93 and 94.

Please let me know if you need additional information.

cc: Carol Kraklan
Sue Doby
Phil Rock
Nancy Presocki

**STATE OF MICHIGAN**

# FAMILY INDEPENDENCE AGENCY

**MEMORANDUM**

**To:** Sue London, Director
SWSS Project

Date: November 1, 1999

**From:** Mary Ann Jensen, Consultant
SWSS Policy
Child and Family Services Administration

**Subject:** Security Module Documentation

We have carefully reviewed the User Requirements document on the October 6, 1999 Security Module (printed October 7, 1999) and have the following clarifications:

1. Page 3, footnote, 2nd line: Add "…as well ***as*** GroupWise…"
2. Page 3, footnote, last line: Add a period at the end of the sentence.
3. Page 7, clerical staff: Says 'need some definitions here' What kind of definitions are needed?
4. Page 7, Level/Function, 1st paragraph, 2nd sentence: This sentence is in error. Clerical level users have access to and update privileges for all cases in their unit except for high profile cases.
5. Page 7, Level/Function, 2nd paragraph: Delete the 'y' in the 2nd word.
6. Page 8, SC-4.1.1: Delete the word 'to'
7. Page 8, SC-4.2, footnote: Access requirements were defined while staff profiles issues were being discussed. What more is needed.
8. Page 9, SC-4.5.1.1, footnote: This requirement is not to be implemented until the system is ready for final acceptance testing. (It's OK that it is not implemented yet.)
9. Page 10, SC-4.6.2.2: Delete the words 'Supervised Adoption' in this requirement.
10. Page 12, SC-4.7.2: There is a reference to Outstanding Issues; however, there is nothing regarding active load numbers in Outstanding Issues.
11. Page 12, SC-4.8: We do not understand what this requirement is trying to say. The references to LOA2 should be deleted as we cannot comment on LOA2 requirements.
12. Page 13, SC-4.11 through 4.16: We believe these should be renumbered as sub-requirements under SC-4.10 (i.e., SC-4.10.1 through SC-4.10.6).
13. Outstanding Issue #14: Add a requirement under SC-4.5 that 'The user's password is to be expired after three months of user inactivity.'

14. Outstanding Issue #15: Modification of the FIA-60. We believe the responsibility for this form resides with ITMS Security Administration.
15. Outstanding Issue #16: MARE access requirements. These appear to be correct.
16. Please review the October 26, 1999 memo, Utilities/Staff Utilities Module Documentation – Addendum 2, and include in this (Security) module any appropriate modifications which may have been caused by that memo.

Security Module Documentation
November 1, 1999
Page –2-

Please note that the requirements being developed on the SWSS/MPS Interface may effect this module.

Please let me know if you need additional information.

cc: Carol Kraklan
Phil Rock
Sue Doby
Nancy Presocki

## 11.2.3 Security, secondary worker

**From:** Mary Ann Jensen
**To:** DSS.BUIS.PALMATIERP, KRAKLANC2
**Date:** 6/1/99 11:23am
**Subject:** log #2822 -Reply -Reply

The supervisor of the secondary worker should have the same update capabilities as the secondary worker. (This Email should be considered an addendum to the 5/24/99 System Security memo.)

Please let me know if we need further discussion.

>>> Carol Kraklan 05/28/99 10:40am >>>
Mary Ann, this is a problem for assigning an adoption worker. The adoption sup. does the assignment and the message about printing a 5S to update CIS with the secondary worker information displays after the adoption sup. assigns the case, but they can not print a 5S.

What should we do?

>>> Paula PALMATIER 05/28/99 10:27am >>>
This was the one where you signed on as lonsberrymsup and tried to print the 5S. lonsberrymsup is the supervisor to the secondary worker (adopt worker). Security program does not give Update capabilities to the sup of the secondary worker.

**CC:** DSS.BUIS.PRESOCKIN

## 11.2.4 Security, profiles, password, flag

3A

STATE OF MICHIGAN
**FAMILY INDEPENDENCE AGENCY**

*MEMORANDUM*

To: Nancy Presocki, Manager
SWSS Development Team

Date: May 24, 1999

From: Mary Ann Jensen, Consultant
SWSS Policy

Subject: System Security

The SWSS Children's Foster Care, Juvenile Justice and Adoption application should be considered a high security risk application. Data is of a very sensitive nature and any inappropriate use of SWSS information can cause major repercussions. After several recent meetings with the Security Office, the SWSS Project Office and the Program Office, it became apparent that there are a number of weaknesses in the security function. The following defines the problems and provides possible solutions. Also, attached are DMB security guidelines.

**Problem 1:** Currently the application only allows for one alternate and one supervisor for each security profile. Access rights (e.g., Juvenile Justice, Children's Foster Care) granted to a user profile are also granted to assigned alternates and supervisors. This can give alternates and supervisors more access rights then they have been authorized to have (or need to have) in their own user profile. For example, if John Smith has been given security administrator access, his alternate and supervisor also have security administrator access.

**Problem 2:** The application allows the security administrator to create multiple profiles for a single user ID. This was designed to allow multiple primary loads to accommodate workers serving multiple programs under distinct load numbers. This creates the need for an unmanageable number of primary workload numbers. This also generates a greater number of profiles for the same worker. The access rights feature of the SWSS application provides the ability to designate multiple program access under one load number so the need for multiple load numbers does not exist.

A related issue is that security coordinators from different counties can make a profile for a worker not located in their county and reset passwords for that worker regardless of the worker's work location. Reports by workload number won't accurately reflect worker's workload.

There is no link between profiles with the same user ID so each profile will need to be deleted. A worker has access to the system as long as there is an active profile. This will make maintenance increasingly difficult and create the potential for profiles to get "lost" in the system.

stem Security
ıy 24, 1999
ıge –2-

38

**lution 1&2**: The application should assign an alternate worker and, if necessary, ɔervisor for each assigned access right. This allows greater control of who can access ɔgrams as alternate/supervisor. The program should verify that the alternate/supervisor ve access rights to the same program they are backing up. For example, Sally Baker has enile justice access, her alternate or supervisor needs to also have juvenile justice access.

:curity Administration will not have any alternate/supervisor options.

low only one profile per user ID.

**oblem 3**: There are no requirements on depth of rotation of unique passwords.

**lution 3**: Password can not be reused until three password change cycles.

**oblem 4**: There is no required password change on initial signon or after a password et. It is important for a user to create his/her own password. Users need to change their ssword if they feel it has been compromised. Generally passwords are reset/established to a ıeric password. The security administrator who established the user or reset the password ɔws the user's password, making it a compromised password.

lution 4: Require a password change on initial signon and after password resets.

**oblem 5**: Currently, there is no limit of failed attempts per user ID.

lution 5: Lock account after the third failed attempt.

**oblem 6**: Application never times out.

**lution 6**: Invoke a time out procedure after 20 minutes of idle time. Oracle will connect and the user would have to re-connect.

**ɔblem 7**: The application only allows security administrators to delete security profiles ıer than make them inactive.

**ution 7**: Add a field to the security profile to indicate user status as active or inactive.

**ɔblem 8**: Central Office needs inquiry access for case information. Is there a provision this?

**ution 8**: This is open for discussion on the best possible solution.

**ɔblem 9**: There is concern regarding access to high profile cases. High profiles cases uld include easily recognized people, e.g., agency staff, public officials, famous people, es receiving media attention. Provisions need to be made to limit access to these cases.

System Security
May 24, 1999
Page –3-

30

**Solution 9**: Allow security administrators to set a flag on the security profile and workers/supervisors to set a flag on the case file. Access would be restricted to case summary and soundex only on these cases so that only the flagged profiles could access the detailed flagged case files.

**Problem 10**: The SWSS application will be collecting confidential medical information on clients. The main concern is about cases with containing information on highly contagious diseases. Cases with in this category need to have medical information restricted.

**Solution 10**: Allow security administers to set a flag on the security profile and workers to set a flag on the case file. Flagged cases would be restricted to case summary. Full access to medical information would be granted to staff with flagged security profiles.

**Problem 11**: Management needs to have a mechanism to monitor staff whose credibility may be questionable.

**Solution 11**: Provide Central Office administrators the ability to establish alerts or audit trails on user Ids. This should be an ad hoc report.

**Problem 12**: It is our understanding that Oracle may have a number of "back door" access points.

**Solution 12**: All points of access need to be found and closed.

Thank you for your attention and cooperation in resolving these issues. Please let me know if we need further discussion.

cc: Sue London
Phil Rock
Sue Doby
Lynn Croxford
Sue Tomes
Carol Kraklan
Cindy Fate

Agencies which accept credit cards for monetary business transaction via Internet or Intranet servers, must consider security techniques, such as SSL or Secure Electronic Transactions (SET). The use of encryption technologies for achieving data privacy, E-mail privacy, user authentication, protection of customer credit cards or establishing private virtual networks must be described and approved via the DMB OIT RAD process (Administrative Procedure 1310.11).

Encrypted data, which is subject to public release and is requested under Public Act 442, the Freedom of Information Act, must be converted back to clear, unencrypted text.

Agencies and Users must comply with current Federal Government regulations on export and import of advanced encryption technology outside the US and Canada.

6.6 PASSWORD POLICY -
Users are expected to handle account privileges in a responsible manner and follow site procedures for the security of their data as well as that of agency systems. All agencies and their network users must follow the password guidelines outlined below. Agencies are responsible for defining and maintaining appropriate methods for file protection and server access control.

A necessary component of agency account management is password assignment policy. Passwords represent a security risk and perhaps are the most vulnerable part of any computer system. Intruders/attackers use sophisticated password guessing programs that involve large dictionary searches and algorithms to discover passwords. The following represent three levels of password security policy (minimum, normal or high) which agencies may choose:

| | MINIMUM SECURITY | NORMAL SECURITY | HIGH SECURITY |
|---|---|---|---|
| password composition | digits (0-9) | Upper (A-Z, lower (a-z) | full 95 ascii |
| password length | 4-6 characters | 4-8 characters | 6-8 characters |
| frequency of change | once per year | twice per year | monthly. |

It is recommended that agencies use high security password profile of a mix of 6-8 alpha and digit ascii characters, but may change user passwords at least once every six months and not reuse those password until 3 password change cycles.

The following are password guidelines to avoid:
- DON'T use common words in proper or reverse spelling
- DON'T use common computer acronyms like SQL, DBMS,
- DON'T use names of famous or fictitious people
- DON'T use your login name in any form (as is, reversed)
- DON'T use your first, middle, or last name in any form
- DON'T use your spouse's or child's name
- DON'T use easily obtained numbers such as telephone, street, social security, etc.

Distribution Date: 1-6-97

Procedure 1410.17

Page -9-

11.2.5 Addendum 2

STATE OF MICHIGAN

# FAMILY INDEPENDENCE AGENCY

***MEMORANDUM***

To: Sue London, Director
SWSS Project

Date: March 20, 2000

From: Mary Ann Jensen, Consultant
SWSS Policy
Child and Family Services Administration

Subject: Security Module Documentation – Addendum 2

Based on discussions with development staff, it is necessary to amend the November 1, 1999 and January 6, 2000 memos on the Security Module. The following revisions are necessary:

1. SC-4.1.1.1 needs to be revised to state: "There ~~is only one~~ **are two** exceptions. Users who are Central Office Security Coordinators **and users who are PROGRAM OFFICE OR P/DC users accessing the Payment Document Control utility** do not need a load number. (See UT-1.8.2.2 and UT-3.4.1.1)

2. Add a new requirement: SC-4.9.7 PROGRAM OFFICE OR P/DC users accessing the Payment Document Control utility are only allowed access to the Payment Document Control utility under this unique user name. These users cannot have access to any other SWSS module, including Utilities under this unique user name. (See PON-3.3.1, LO-4.5.2, and LO-4.5.3)

3. Add a new requirement: SC-4.12 Payments ONLINE! REQUIREMENTS:

4. Add a new requirement: SC-4.12.1 PROGRAM OFFICE OR P/DC users do not require a security level to access the Payment Document Control utility.

5. Add a new requirement: SC-4.12.2 PROGRAM OFFICE OR P/DC users must not be permitted to become SWSS Security Coordinators under this unique user name.

Please let me know if you need additional information.

cc: Nancy Presocki
Carol Kraklan
Phil Rock
Sue Doby

11.2.6 Memo March 31, 2000

**STATE OF MICHIGAN**

## FAMILY INDEPENDENCE AGENCY

**MEMORANDUM**

**To:** Sue London, Director
SWSS Project

Date: March 31, 2000

**From:** Mary Ann Jensen, Consultant
SWSS Policy
Child and Family Services Adminstration

**Subject:** Log In, Security and Utility Module Documentation

Based on discussions and inclusion of the Payment Exception process (Payment Document Control utility), the above Modules required modifications. The following requirements have be added or modified and posted to on the Web:

1. LO requirements: LO-4.5.1 and LO-4.5.3.
2. Security requirements:
   - SC-4.1.1.1
   - SC-4.7.1
   - SC-4.9.6.1.1
   - SC-4.9.7
   - SC-4.12.1
3. Utility requirements:

| | | |
|---|---|---|
| • UT-1.1.1.7 | UT-1.2.1 | UT1.2.2 |
| • UT-1.5.1.5 | UT-1.5.1.5.1 | UT-1.5.1.5.2 |
| • UT-1.5.1.5.3 | UT-1.5.4.1 | UT-1.8.2.2 |
| • UT-1.8.3.3 | UT-3.4.1.1 | |

These changes have been reviewed and approved. Please let me know if you need additional information.

cc: Carol Kraklan
Sue Doby
Phil Rock
Nancy Presocki

11.2.7 Addendum 6

**STATE OF MICHIGAN**

## FAMILY INDEPENDENCE AGENCY

**MEMORANDUM**

**To:** Sue London, Director
SWSS Project

Date: July 20, 2000

**From:** Mary Ann Jensen, Consultant
SWSS Policy
Child and Family Services Administration

**Subject:** Security Module Documentation - Addendum 6

It is necessary to amend the Security Module Documentation memos of November 1, 1999, January 6, 2000, March 20 and 31, 2000 and June 5 and 15, 2000. After focussed testing (SER #535) and discussions with development staff, it was noted that the following clarification is needed:

SC-4.6.3.1 must be modified to delete "Active-Ac" (350). (There is not a method of accepting a case without assigning it to a staff member.)

Please let me know if you need additional information.

cc: Carol Kraklan
Phil Rock
Sue Doby
Nancy Presocki

11.2.8 Addendum 8

**STATE OF MICHIGAN**
**FAMILY INDEPENDENCE AGENCY**

**MEMORANDUM**

**To:** Sue London, Director
SWSS Project

Date: August 28, 2000

**From:** Mary Ann Jensen, Consultant
SWSS Policy
Child and Family Services Administration

**Subject:** Security Module Documentation - Addendum 8

It is necessary to amend the Security Module Documentation memos of November 1, 1999, January 6, 2000, March 20 and 31, 2000, June 5 and 15, 2000 and July 20 and 27, 2000. After focussed testing (SER #965) and discussions with development staff, it was noted that the following clarification is needed:

SC-4.6.6 must be rewritten as follows: "**Access to the Payment module must be view only if the selected case has been assigned one of the following legal status codes: 'Court Ward Supervised Adoption' (43), 'OTI-Delinquent' (47), 'OTI-Neglect' (48), 'OTI-Adoption' (49), or 'Non-Ward Delinquent Petition Filed' (50)**."
A new requirement is needed: SC-4.6.6.1 "Access to the Payment module must be view only if the current case state is not one of the following: 'Active' (200), 'Active-As' (250), or 'Active-R' (450)."
A new requirement is needed: SC-4.6.6.2 "If the case is closed (case state = 'Closed' (600), the worker's supervisor(s) have update capability. Other users can view only."

Please let me know if you need additional information.

cc: Carol Kraklan
Phil Rock
Sue Doby
Nancy Presocki

11.2.9 Addendum 7

**STATE OF MICHIGAN**

## FAMILY INDEPENDENCE AGENCY

**MEMORANDUM**

**To:** Sue London, Director
SWSS Project

Date: July 27, 2000

**From:** Mary Ann Jensen, Consultant
SWSS Policy
Child and Family Services Administration

**Subject:** Security Module Documentation - Addendum 7

It is necessary to amend the Security Module Documentation memos of November 1, 1999, January 6, 2000, March 20 and 31, 2000, June 5 and 15, 2000 and July 20, 2000. After focussed testing (SER #535) and discussions with development staff, it was noted that the following clarification is needed:

1. SC-4.6.6 must be modified to delete "Active-Ac" (350). (There is not a method of accepting a case without assigning it to a staff member.)

Please let me know if you need additional information.

cc: Carol Kraklan
Phil Rock
Sue Doby
Nancy Presocki

STATE OF MICHIGAN

# FAMILY INDEPENDENCE AGENCY

MEMORANDUM

**To:** Sue London, Director
SWSS Project

Date: December 21, 2000

**From:** Mary Ann Jensen, Consultant
SWSS Policy
Child and Family Services Administration

**Subject:** Security Module Documentation - Addendum 9

It is necessary to amend the Security Module Documentation memos of November 1, 1999, January 6, 2000, March 20 and 31, 2000, June 5 and 15, 2000, July 20 and 27, 2000 and August 28, 2000. After focussed testing (SER #1559) and discussions with development staff, it was noted that the following clarifications are needed:

1. Add a new requirement: (SC-4.8.1.1?) There is one exception. A PROGRAM OFFICE OR P/DC user must be allowed access to the Payments Online! Module when s/he enters the log numbers of a confidential case from the Utilities module (after selecting the P/DC Modification action).
2. SC-4.7.1 must be modified to state: "…. user accessing the Payment Document Control utility **or the P/DC Modification action**, ….."
3. SC-4.9.7 must be modified to state: "…. users accessing the Payment Document Control utility **(or the P/DC Modification action)** are only allowed access to the Login Module, Utilities Module, **the Payments Module,** and the Payment Document Control utility under this unique user name. …… These users use the Utilities module to change their own password and access the Payment Document Control utility **or the P/DC Modification action (the Payments Module)** ….."

Note: This change is not required for the go/no go decision on the Kalamazoo pilot. It is needed before Statewide implementation begins.

Please let me know if you need additional information.

cc: Carol Kraklan
Sue Doby

Beth Dean

# 12 TEST PLAN CREATED BY POLICY

## 12.1 Test Plan Created by SWSS Development

### Test Plan – SWSS Utilities

Matthew D. Miller

Process Accessibility

- All valid SWSS workers are allowed, at least, some level of access to Utilities. A case does **not** have to be selected in order to execute the Utilities process.
- Central Office Security Coordinators and Local Office Security Officers are the only types of workers allowed access to the Add Staff Profile and Inactivate Staff Profile functions. All SWSS workers are allowed access to the Ticklers, Change Staff Profile, and Reconciliation functions.
- Non-security coordinators may only change passwords for their own worker records. They must correctly specify their current (or "Old") password and enter their new password twice before any password changes will be applied to their Oracle account.
- Central Office Security Coordinators may change all other worker data fields on all four screens for all workers in the State Of Michigan. However, when they change another worker's password, they will **not** be required to enter a current password. They will just need to correctly enter the new password twice. Also, Central Office Security Coordinator worker records are not accessible or visible from SWSS Utilities. Their records are maintained outside of the system. Central Office Security Coordinators are also the only workers allowed to create Local Office Security Coordinators.
- Local Office Security Coordinators are assigned county-district combinations that limit which worker records they are allowed to maintain. The only worker records they will see will be workers who are assigned an active load number, which contains one of the county-district combinations, assigned to the coordinator. The Local Office Security Coordinator may then change any worker data fields on all four screens for all of these workers, except their own record. The only data a coordinator may change in his/her own record is his/her password. Coordinators must specify their current password when changing their own record; otherwise they only need to enter a new password twice when modifying other worker records. On the fourth screen, Local Office Security Coordinators may **not** change the Security Administration check box or any county-district combinations for any worker records.
- If the worker being modified is assigned to the Adoption program and given a Supervisor or higher security level, it is possible for a Central/Local Office Security Coordinator to assign a list of counties to the selected worker. These counties represent which counties the worker "covers" for Adoption Supervision.
- Corrections Mode does not apply to the Utilities process.
- If an existing worker's name fields are changed, the original name is written to a worker name history database table (worker_name_hist). There is currently no mechanism for viewing this name history.

10/12/9812:54 PM 330 1

12.2

- When changing a worker's load number, a prompt should come up asking if the new load is to be added to the worker's profile, or if the new load number is meant to replace the current load number.
  - If the former, the load number should become a new valid load number for the worker.
  - If the latter, the database is scanned for active cases attached to the old load.
    - If any cases are found, the user is asked to assign different active load numbers to those cases. Otherwise, the load number change is made.
  - Carefully note that adding any new load numbers to a workers profile is meant to be a part of the Change Staff Profile function, **not** the Add New Staff Profile function.
- Maximum field lengths:
  - Last name = 19 characters
  - First name = 12 characters
  - Middle = 1 character
  - Suffix = 3 characters
  - Username = 30 characters
  - Password = 30 characters (with a minimum of 6 characters)
  - Section, Unit and Worker numbers are limited to two digits
  - Address Line 1 = 60 characters
  - Address Line 2 = 60 characters
  - City = 30 characters
  - Zipcode = 5 digits
  - Zip Plus = 4 digits
  - Phone number = 10 digits
  - Phone extension = 5 digits
- The Inactivate Staff Profile function is first used to inactivate load numbers assigned to a worker (especially if the worker has been assigned multiple load numbers). It is not until the worker's last active load number is inactivated that a worker will be denied access to the SWSS application.
- The user should not be allowed to Inactivate a worker load number if any active case is still attached to it. If a worker's last load number is inactivated, the user should be asked if they wish to eliminate the worker's Oracle account.

Case Functionality

- A valid SWSS case must be selected before Reconciliation may be executed. If one hasn't been selected, user should be prompted to "jump" to the Case Listing process for case selection.
- Only Juvenile Justice, Foster Care, and Adoption cases should be allowed to be reconciled. Also, those cases must have a status of either Unregistered or Registered.

**MEMORANDUM**

**To:** Sue London, Director
SWSS Project

Date: June 5, 2000

**From:** Mary Ann Jensen, Consultant
SWSS Policy
Child and Family Services Administration

**Subject:** Security Module Documentation - Addendum 4

It is necessary to amend the Security Module Documentation memos of November 1, 1999, January 6, 2000, and March 20 and 31, 2000. After discussions with development staff, it was noted that SC-4.6.2.2 and SC-4.6.2.3 must be modified to resolve the discrepancies between this Module and the M.A.R.E. Module:

SC-4.6.2.2 The current user must be granted access to MARE if the current legal status assigned to the selected case is either "Permanent Court Ward" (41), "MCI Ward" (44) or "Dual Ward" *(52, 91, 93 or 94)* ***and*** the goal code assigned to the case is "Adoption" ~~(CommCare)~~(10).

SC-4.6.2.3 The current user must be granted access to MARE regardless of the legal status if the case state is currently "Active-As" (250) or Registered-As" (275) ***and*** the goal code assigned to the case is "Adoption" ~~(CommCare)~~(10).

Please let me know if you need additional information.

cc: Carol Kraklan
Phil Rock
Sue Doby
Nancy Presocki

**STATE OF MICHIGAN**

## FAMILY INDEPENDENCE AGENCY

**MEMORANDUM**

**To:** Sue London, Director
SWSS Project

Date: June 15, 2000

**From:** Mary Ann Jensen, Consultant
SWSS Policy
Child and Family Services Administration

**Subject:** Security Module Documentation - Addendum 5

It is necessary to amend the Security Module Documentation memos of November 1, 1999, January 6, 2000, March 20 and 31, 2000 and June 5, 2000. After focussed testing and discussions with development staff, it was noted that the following clarifications are needed:

2. Add a sub-requirement to SC-4.6.2.1: The message must state "Access to M.A.R.E. is denied; child is already in an adoptive placement."
3. Add a sub-requirement to SC-4.6.2.2: The message must state "Access to M.A.R.E. is denied; the goal for this permanent ward is not adoption."
4. Add a sub-requirement to SC-4.6.2.3: The message must state "Access to M.A.R.E. is denied; this temporary ward's case has not been assigned to an adoption worker."

Please let me know if you need additional information.

cc: Carol Kraklan
Phil Rock
Sue Doby
Nancy Presocki

# 12 OUTSTANDING ISSUES

12.1 The following items require a decision or some direction from Policy staff:

1 Define the requirement, “Central Office needs inquiry access for case information”. Mary Ann Jensen is looking into providing more information on this requested feature.
2 How will central office staff view finalized adoption cases that are supposed to be unavailable to local office staff?

12.2 The following items require a decision by ITMS Staff

3 Central Office Security Coordinator profiles must be maintained outside of the SWSS application (a requirement requested by the security office), but the database team is requesting the SWSS development team maintain some of the data, and this must be resolved. (UT-3.1.1 Before any staff profiles can be created, the Oracle DBA must first create a Central Office Security Coordinator profile. The user of this profile can then create Local Office Security Coordinator profiles whose users can assist in creating the standard SWSS profiles for the county-districts that they have been assigned to.)
4 The SWSS/StaffProfiles application does not expire a user’s password after three or six months of user inactivity. **Answer: Yes, SWSS ought to do this!**
5 The FIA-60 requires modifications and the status of those changes and the ultimate responsibility of that form are unclear.
6 The MARE access requirements (SC-4.6.2 and below) ought to be reviewed once MARE has been reviewed.

# 13 ATTACHMENTS

13.1 A: List of SWSS Module Prefixes

## MODULE PREFIXES TO BE USED FOR REQUIREMENTS

| MODULE | TABLE |
|---|---|
| CASE LISTING | CL |
| MAIN MENU | MM |
| CASE REGISTRATION | CR |
| CHILD INFO | CI |
| MEMBER INFO | MI |
| LEGAL | LE |
| FUNDING DETERMINATION | FD |
| PLACEMENT | PL |
| PAYMENT | PA |
| EDUCATION | ED |
| MEDICAID | MA |
| MEDICAL PASSPORT | MP |
| FIVE DAY PACKET | FP |
| COMMENTS | CO |
| CASE SUMMARY | CS |
| CASE CLOSING | CC |
| MARE | MR |
| ADOPTION ACTIVITY | AA |
| REPORT GENERATION | RG |
| TICKLERS | TI |
| PROVIDERS | PR |
| UTILITIES | UT |
| LOGIN | LO |
| SECURITY | SC |
| PRINT133A | P1 |
| PRINT5S | 5S |
| ACTION SUMMARY | AS |
| PURCHASE OF SERVICE | PU |
| PS XFER | PX |
| CONVERSION | CV |
| SOUNDEX | SO |
| COMMON | CM |
| RECONCILIATION | JTL |